

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-337736

(43)Date of publication of application : 28.11.2003

(51)Int.Cl. G06F 12/00
G06F 3/06
G06F 12/14
H04L 9/10

(21)Application number : 2002-144942

(71)Applicant : HITACHI LTD

(22)Date of filing : 20.05.2002

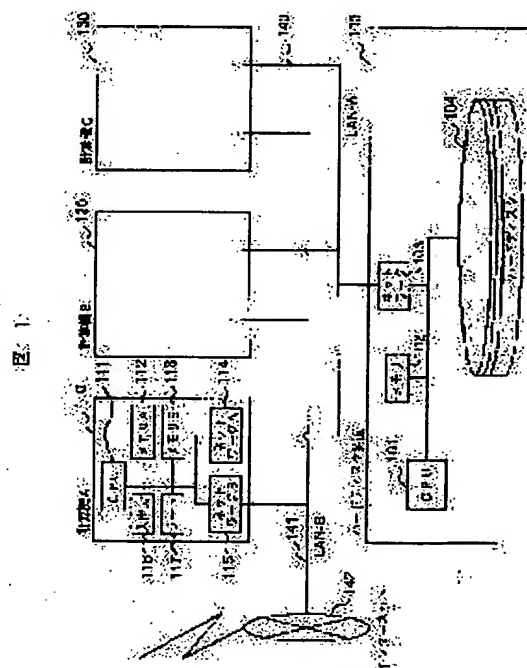
(72)Inventor : KIMURA SHINJI
KARASAKI SADAJI
SATO MASAHIDE
OSHIMA SATOSHI

(54) COMPUTER, HARD DISK DEVICE, DISK DEVICE SHARING SYSTEM CONSTRUCTED OF A PLURALITY OF COMPUTERS AND SHARED HARD DISK DEVICE, AND SHARING METHOD FOR DISK DEVICE USED IN THE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize safety data communication between respective computers and a shared hard disk device mutually connected via a network and to provide a disk device sharing system reducing the operation cost required for maintenance of the computers.

SOLUTION: Two OS are mounted on a single computer. One is a first OS executing an application program, while the other is a second OS processing communication with the shared hard disk device. Access from the application program to the shared hard disk device is always passed through the second OS, and control is carried out so that direct access from the application program and the first OS to the hard disk device is not allowed.



LEGAL STATUS

[Date of request for examination]

13.07.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-337736

(P2003-337736A)

(43)公開日 平成15年11月28日(2003.11.28)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 12/00	5 4 5	G 0 6 F 12/00	5 4 5 A 5 B 0 1 7
	5 3 7		5 3 7 H 5 B 0 6 5
3/06	3 0 1	3/06	3 0 1 C 5 B 0 8 2
	3 0 4		3 0 4 H 5 J 1 0 4
12/14	3 2 0	12/14	3 2 0 A

審査請求 未請求 請求項の数20 O L (全 12 頁) 最終頁に続く

(21)出願番号 特願2002-144942(P2002-144942)

(22)出願日 平成14年5月20日(2002.5.20)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 木村 信二

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72)発明者 唐崎 貞二

神奈川県海老名市下今泉810番地 株式会

社日立製作所インターネットプラットフォーム事業部内

(74)代理人 100068504

弁理士 小川 勝男 (外2名)

最終頁に続く

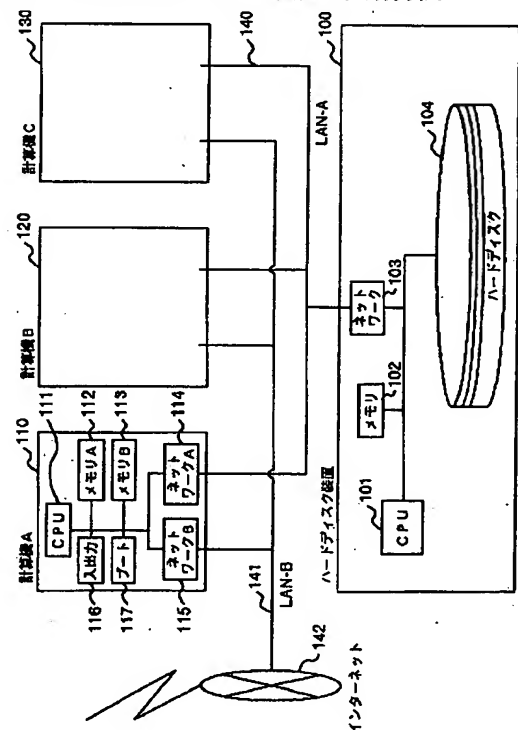
(54)【発明の名称】 計算機、ハードディスク装置、複数の該計算機及び共有ハードディスク装置から構成されるディスク装置共有システム、及び該共有システムにおいて利用されるディスク装置の共有方法

(57)【要約】

【課題】 複数の計算機と共有ハードディスク装置がネットワークで相互接続される環境において、各計算機とハードディスク装置間の安全なデータ通信を実現し、計算機用のメンテナンスに要する運用コストの低減するディスク装置共有システムを提供する。

【解決手段】 1台の計算機上に2つのOSを搭載する。1つは、アプリケーションプログラムを実行する第一のOS、もう一つは共有するハードディスク装置との通信処理を行う第2のOSである。アプリケーションプログラムからの共有ハードディスク装置へのアクセスは、必ず第二のOSを経由させ、アプリケーションプログラム及び第一のOSからはハードディスク装置に直接アクセスできないよう制御する。

図 1



【特許請求の範囲】

【請求項 1】 アプリケーションプログラムを実行する複数の計算機と、前記複数の計算機により共用されるハードディスク装置と、前記複数の計算機と前記ハードディスク装置がネットワークにより相互接続されるディスク装置共有システムにおいて、

前記複数の計算機は、前記アプリケーションプログラムを実行する第 1 のオペレーティングシステムと、前記計算機と前記ハードディスク装置間の通信処理を実施する第 2 のオペレーティングシステムとを備え、前記第 1 のオペレーティングシステムと第 2 のオペレーティングシステムとは相互に独立して実行することを特徴とするディスク装置共有システム。

【請求項 2】 前記第 1 のオペレーティングシステムは前記計算機においてユーザにより実行される前記アプリケーションプログラムを制御するユーザ処理 OS であり、前記第 2 のオペレーティングシステムは、前記計算機と前記ハードディスク装置間の通信処理を制御する通信処理 OS であり、前記複数の計算機は、内臓ディスクを備えないことを特徴とする請求項 1 に記載のディスク装置共有システム。

【請求項 3】 前記ハードディスク装置は、鍵生成データを備え、前記複数の計算機と前記ハードディスク装置間の通信データを暗号化することを特徴とする請求項 2 に記載のディスク装置共有システム。

【請求項 4】 請求項 3 記載のディスク装置共有システムにおいて、

前記複数の計算機は、前記ネットワークを経由して前記ハードディスク装置から前記第 1 のオペレーティングシステム、第 2 のオペレーティングシステム、及び前記アプリケーションプログラムをプログラムブートすることを特徴とする請求項 3 に記載のディスク装置共有システム。

【請求項 5】 前記複数の計算機は、前記ネットワークを経由して前記ハードディスク装置から前記第 1 のオペレーティングシステム及び第 2 のオペレーティングシステムをプログラムブートし、前記アプリケーションプログラムをデータとして、前記ハードディスク装置からロードすることを特徴とする請求項 3 に記載のディスク装置共有システム。

【請求項 6】 前記ハードディスク装置は、前記複数の計算機と前記ハードディスク装置間の通信データを暗号化するために、前記鍵生成データに基づき鍵データを作成し、前記プログラムブート時に前記複数の計算機に対し前記鍵生成データ、或いは前記鍵データを配信することを特徴とする請求項 5 に記載のディスク装置共有システム。

【請求項 7】 第 1 の OS と第 2 の OS を備えた計算機から構成され、該第 1 の OS と第 2 の OS は相互に独立して実行し、前記計算機はユーザにより利用されるアプリ

ケーションソフト及び通信処理部を備え、前記ユーザが前記第 1 の OS の制御により前記アプリケーションソフトを実行した結果、得られるデータを前記通信処理部が備える暗号処理ユニットにて前記第 2 の OS の制御により暗号化し、前記第 2 の OS により制御されるネットワーク部を介して前記暗号化されたデータを外部インターフェースに接続されるハードディスク装置に送信することを特徴とする計算機。

【請求項 8】 請求項 7 記載の計算機において、前記第 2 の OS は前記通信処理部を制御し、前記暗号処理ユニットは前記ハードディスク装置から配信された鍵生成データに基づき鍵データを作成し、前記データの暗号化を実施することを特徴とする計算機。

【請求項 9】 請求項 8 記載の計算機において、前記第 1 の OS は前記アプリケーションソフトを制御するユーザ処理 OS であり、前記第 2 の OS は前記ネットワーク部を介して前記ハードディスク装置と前記暗号化された前記データの通信を実施する通信処理 OS であることを特徴とする計算機。

【請求項 10】 CPU、メモリ、ハードディスクユニット及びネットワーク部を備えるハードディスク装置から構成され、

前記 CPU はブート処理部、認証プログラムユニット、通信処理部及び前記ハードディスクユニットを制御するディスク管理部を含み、

前記通信処理部は、暗号処理ユニット及び鍵生成データを備え、

前記認証プログラムユニットは前記ネットワーク部を介して接続されている複数の計算機の各々が有するハードウェア情報及び前記計算機を管理する使用者情報を保持し、

前記ハードディスクユニットは複数の領域を備え、該複数の領域には前記複数の計算機毎の前記ハードウェア情報が格納され、

前記暗号処理ユニットは、前記計算機から送信されるブート要求を前記ブート処理部にて処理した後、前記鍵生成データに基づき鍵データを作成し、前記ハードウェア情報に前記鍵生成データ或いは鍵データを付加して前記ブート要求を発信した前記計算機に対し配信することを特徴とするハードディスク装置。

【請求項 11】 請求項 10 記載のハードディスク装置において、

前記ハードウェア情報は前記計算機毎に格納されているユーザ処理 OS、通信処理 OS、及びユーザにより利用されるアプリケーションプログラムを含み、前記使用者情報はユーザを識別する為の認証情報であることを特徴とするハードディスク装置。

【請求項 12】 請求項 11 記載のハードディスク装置において、

前記認証情報は、前記計算機を使用するユーザ名、該ユ

ーザのパスワード、及び該ユーザが利用しているデータ格納用ディスクの情報であることを特徴とするハードディスク装置。

【請求項 13】請求項 10 記載のハードディスク装置において、

前記鍵データは前記暗号処理ユニットが備える鍵データ部において作成され、前記鍵データ部は計算機を識別する為の固有データ及び暗号化情報を保持することを特徴とするハードディスク装置。

【請求項 14】請求項 13 記載のハードディスク装置において、

前記固有データ及び暗号化情報は前記計算機のネットワークアドレス、前記鍵生成データ、前記鍵データ、及び前記鍵データの生成時間を含む情報であることを特徴とするハードディスク装置。

【請求項 15】請求項 10 記載のハードディスク装置において、

前記ディスク管理部の制御に従い、前記計算機から前記送信される暗号化された通信データを前記通信処理部が処理し、前記ハードディスクユニットが有する前記複数の領域の内、何れかの領域に前記暗号化された通信データを格納することを特徴とするハードディスク装置。

【請求項 16】請求項 15 記載のハードディスク装置において、

さらに、前記ディスク管理部の制御に従い、前記計算機から送信される前記暗号化された通信データを前記暗号処理ユニットが有する前記鍵データを使用し、暗号化されていない元データに戻し、前記複数の領域の内、何れかの領域に該元データを格納することを特徴とするハードディスク装置。

【請求項 17】複数の計算機と、該複数の計算機により共用されるハードディスク装置と、該複数の計算機と前記ハードディスク装置がネットワークにより相互接続される計算機システムにおいて、

前記計算機システムがブート処理するステップと、前記ブート処理の後、前記計算機はユーザによる認証 ID の入力後、認証データを作成し前記ハードディスク装置に対し、送信するステップと、

前記ハードディスク装置にて前記認証データの認証処理を実施し、前記複数の計算機に対し、前記ハードディスク装置が備える暗号処理部が鍵データを作成するステップと、

前記計算機の実行に必要と成るオペレーティングシステム、前記ユーザにより利用されるアプリケーションソフトと共に前記鍵データを前記計算機に対し配信するステップとを含むことを特徴とするディスク装置の共有方法。

【請求項 18】請求項 17 記載のディスク装置の共有方法において、

前記ハードディスク装置は、鍵生成データ及び鍵データ

部を備え、前記作成するステップにおいて、前記鍵生成データに基づいて前記鍵データが作成され、前記鍵データ部は前記複数の計算機と前記ハードディスク装置間の通信データを前記暗号処理部にて暗号化する際に必要な前記鍵データを格納することを特徴とするディスク装置の共有方法。

【請求項 19】請求項 18 記載のディスク装置の共有方法において、

前記オペレーティングシステムは、ユーザ処理 OS 及び通信処理 OS を含み、前記配信するステップにおいて、前記計算機に対し、前記鍵生成データ或いは鍵データが前記オペレーティングシステム及びアプリケーションソフトと共に送信されることを特徴とするディスク装置の共有方法。

【請求項 20】請求項 17 記載のディスク装置の共有方法において、

さらに前記鍵データを用いて、前記計算機は前記ユーザにより利用されるアプリケーションソフトを実行した結果、得られるデータを暗号化し前記ハードディスク装置に対し前記ネットワークを介して転送するステップを含むことを特徴とするディスク装置の共有方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数の計算機がハードディスク装置を共有するディスク装置共有システムに関し、特に、該共有システムにおいて利用される当該ディスク装置の共有方法に関する。

【0002】

【従来の技術】計算機は使用する形態により分類できるが、ユーザが文書処理等のアプリケーションプログラムで使用するパソコン等の計算機はクライアント計算機、また、Webサーバやメールサーバのように複数のユーザにサービスを提供するためのアプリケーションプログラムを実行する計算機はサーバ計算機と呼ばれる。

【0003】このようなクライアント計算機やサーバ計算機は、基本的な構成は同じであり、高性能な CPU、大容量のメモリ、大容量なハードディスク装置、及び高速なグラフィック装置等を搭載している。オペレーティングシステム (OS)、アプリケーションプログラムやユーザデータ等はストレージとしてのハードディスク装置に格納される。

【0004】また、ネットワークコンピュータと呼ばれる計算機の形態があるが、これは、OS やアプリケーションプログラムを格納するハードディスク装置を各クライアント計算機に備えず、サーバ計算機上でアプリケーションプログラムを実行し、その表示のみの機能を備えることによって、低価格、低機能化した計算機である。

【0005】また、複数の計算機でハードディスク装置を共有する方法として、Ethernet (登録商標) のようなネットワーク上の通信プロトコルに、ハードデ

ディスク装置にアクセスするためのSCSIプロトコルを使う、iSCSI (Internet Small Computer Systems Interface) プロトコルが知られている。

【0006】計算機がプリブート／リモートブート機能を備える場合は、OSやアプリケーションプログラムのロードを、サーバ計算機から行えるため、前記iSCSIプロトコルを使ったハードディスク装置の共有と組み合わせることによって、各計算機にハードディスク装置を備える必要のない計算機を実現できる。このような計算機はディスクレス計算機と呼ばれる。

【0007】

【発明が解決しようとする課題】上述したディスクレス計算機は、OS、アプリケーションプログラム及びユーザデータを、ネットワークにより共有したハードディスク装置に格納できるためのインストール、バージョンアップ、バックアップに伴う作業を簡素化できる利点がある。

【0008】しかし、Ethernet (登録商標) のようなネットワークを使用して、計算機とストレージを接続する形態では、ネットワーク上のデータは盗聴可能であり安全でないという問題がある。ここで、盗聴とはハッカー等によるデータの改変の事である。

【0009】また、複数のディスクレス計算機と共有ハードディスク装置がネットワークで接続される形態では、1台のディスクレス計算機の管理者権限が奪われると、同じネットワーク上の計算機及びハードディスク装置内におけるデータの安全性が失われるという問題がある。

【0010】本発明の目的は、複数の計算機と共有ハードディスク装置がネットワークを介して相互接続される環境において、安全なデータ通信を実現し、計算機のメンテナンスに要する運用コストの低減を実現するディスク装置共有システムを提供する事にある。

【0011】

【課題を解決するための手段】前記課題を解決し、上述した目的を達成するために、本発明は1台の計算機上に2つのOSを搭載する。1つは、アプリケーションプログラムを実行する第1のOS、もう一つは共有するハードディスク装置との通信処理を行う第2のOSである。本発明によれば、アプリケーションプログラムを実行する第1のOSの管理者権限を不正なプログラムにより奪われても、第2のOSの管理者権限を奪わなければ、共有ハードディスク装置にアクセスすることはできない。

【0012】さらに、本発明によれば、第2のOSと共有ハードディスク装置間の通信データを暗号化することによって、他の計算機からのデータ盗聴を防ぐことが可能になる。各計算機のOSをプリブート／リモートブート機能を使って、共有ハードディスク装置から配布するときに、通信データの暗号化に必要な鍵データを、リモ

ートブートするOSといっしょに配布することによって、各計算機に鍵データを保存する必要がないため、鍵データの盗難を防ぐことが可能である。

【0013】さらに、配布する鍵データは第2のOSが管理するメモリ領域に保存し、第1のOSからアクセスできないようにすることによって、安全性を高めることができる。

【0014】

【発明の実施の形態】本発明の実施の形態について説明する。尚、実施例を示す各図における同一符号は同一物または相当物を示す。以下、図面を用いて本発明の実施の形態について説明する。図1は本発明の実施の形態におけるディスク装置共有システムを使用した計算機環境の構成を示す図である。

【0015】ハードディスク装置100は、計算機A110、計算機B120、計算機C130のOS、アプリケーションプログラム及びユーザデータを格納するための共有ハードディスク装置である。当該ハードディスク装置はCPU101、メモリ102、ネットワークデバイス103及び、ハードディスクデバイス104で構成される。ハードディスクデバイス104には、各使用者のOS、アプリケーションプログラム及びユーザデータが格納されているものとする。

【0016】計算機A110、計算機B120、計算機C130は使用者A、B、Cが使用する計算機である。それぞれの計算機は、CPU111、メモリA112、メモリB113、ネットワークデバイスA114、ネットワークデバイスB115、入出力デバイス116、ブート制御回路117から構成される。各計算機に内蔵されているネットワークデバイスA114は、LAN-A140を経由して、ハードディスク装置100に接続される。また、ネットワークデバイスB115はLAN-B141を経由して、インターネット142に接続されているものとする。また、入出力デバイス116は、キーボードと表示装置で構成されるものとする。

【0017】本発明の実施形態による図1に示すディスク装置共有システムは、以下の項目(a)から(f)の特徴を有するディスク装置共有システムとして提供することも可能である。

【0018】(a)アプリケーションプログラムを実行する複数の計算機と、前記複数の計算機により共用されるハードディスク装置と、前記複数の計算機と前記ハードディスク装置がネットワークにより相互接続されるディスク装置共有システムにおいて、前記複数の計算機は、前記アプリケーションプログラムを実行する第1のオペレーティングシステムと、前記計算機と前記ハードディスク装置間の通信処理を実施する第2のオペレーティングシステムとを備え、前記第1のオペレーティングシステムと第2のオペレーティングシステムとは相互に独立して実行することを特徴とするディスク装置共有シ

システム。

【0019】(b)前記第1のオペレーティングシステムは前記計算機においてユーザにより実行される前記アプリケーションプログラムを制御するユーザ処理OSであり、前記第2のオペレーティングシステムは、前記計算機と前記ハードディスク装置間の通信処理を制御する通信処理OSであり、前記複数の計算機は、内臓ディスクを備えないことを特徴とする、上記(a)に記載のディスク装置共有システム。

【0020】(c)前記ハードディスク装置は、鍵生成データを備え、前記複数の計算機と前記ハードディスク装置間の通信データを暗号化することを特徴とする、上記(b)に記載のディスク装置共有システム。

【0021】(d)前記複数の計算機は、前記ネットワークを経由して前記ハードディスク装置から前記第1のオペレーティングシステム、第2のオペレーティングシステム、及び前記アプリケーションプログラムをプログラムブートすることを特徴とする、上記(c)に記載のディスク装置共有システム。

【0022】(e)前記複数の計算機は、前記ネットワークを経由して前記ハードディスク装置から前記第1のオペレーティングシステム及び第2のオペレーティングシステムをプログラムブートし、前記アプリケーションプログラムをデータとして、前記ハードディスク装置からロードすることを特徴とする、上記(c)に記載のディスク装置共有システム。

【0023】(f)前記ハードディスク装置は、前記複数の計算機と前記ハードディスク装置間の通信データを暗号化するために、前記鍵生成データに基づき鍵データを作成し、前記プログラムブート時に前記複数の計算機に対し前記鍵生成データ、或いは前記鍵データを配信することを特徴とする、上記(e)に記載のディスク装置共有システム。

【0024】図2は本発明の実施の形態における図1の計算機A110、計算機B120、計算機C130で動作するソフトウェアの構成を示したものである。

【0025】各計算機では、使用者が使用するアプリケーションプログラム204を実行するユーザ処理OS200と、ハードディスク装置100との通信を処理する通信処理OS201とが独立して実行する。独立して実行するとは、2つのOSが計算機110、120、130の資源であるメモリや入出力デバイスを分割して利用し、互いの実行が他に影響を与えないことを言う。この複数のOSを実行するための処理は複数OS処理202で行う。1つの計算機で複数のOSを独立に実行する技術は、特開平11-149385号公報(以下、文献1と称する)に開示されている。上記文献1によれば、ユーザ処理OS200と通信処理OS201を独立実行でき、ユーザ処理OS200が障害で停止した場合でも、通信処理OS201は継続して動作できる。

【0026】ユーザ処理OS200は、LAN-B141を経由してインターネットに接続するためのネットワーク処理206と、アプリケーションプログラム204からのディスク装置へのアクセスを行う際、ディスク装置に対し、通常、送信する制御コマンドなどを通信プロトコルに変換するための仮想ディスク処理207を備える。仮想ディスク処理207は、複数OS処理202が提供するOS間通信処理203を使い、もうひとつのOS201で実行される通信処理205に通信データを送る。通信処理205は、必要に応じて、暗号処理209で通信データの暗号化を行い、通信処理OS201のネットワーク処理208によりLAN-A140を経由して、ハードディスク装置100と通信処理を行う。計算機110、120、130とハードディスク装置100の通信データを暗号化する場合は、メモリA112(図1)に格納した鍵生成データ210から求めた鍵データ211を用いて暗号化した通信データで通信を行うものとする。ここで、上述した通信データの暗号化は、公開暗号鍵方式に準拠している。通信処理OS201、複数OS処理203、鍵生成データ210はメモリA112に格納され、ユーザ処理OS200はメモリB113に格納する。これらの処理ソフトウェア及びデータは、計算機110、120、130の電源を入れたときに、ブート制御回路117に格納されたプリブート/リモートブート機能により、ネットワークデバイスA114を使い、LAN-A140を経由して、ハードディスク100からネットワークブートによりロードされる。

【0027】本発明の図2に示すソフトウェアの構成に基づき、動作する図1の各計算機A110、B120、C130は、以下の項目(I)から(III)の特徴を有する計算機として提供することも可能である。

【0028】(I)第1のOSと第2のOSを備えた計算機から構成され、該第1のOSと第2のOSは相互に独立して実行し、前記計算機はユーザにより利用されるアプリケーションソフト及び通信処理部を備え、前記ユーザが前記第1のOSの制御により前記アプリケーションソフトを実行した結果、得られるデータを前記通信処理部が備える暗号処理ユニットにて前記第2のOSの制御により暗号化し、前記第2のOSにより制御されるネットワーク部を介して前記暗号化されたデータを外部インターフェースに接続されるハードディスク装置に送信することを特徴とする計算機。

【0029】(II)前記第2のOSは前記通信処理部を制御し、前記暗号処理ユニットは前記ハードディスク装置から配信された鍵生成データに基づき鍵データを作成し、前記データの前記暗号化を実施することを特徴とする、上記(I)に記載の計算機。

【0030】(III)前記第1のOSは前記アプリケーションソフトを制御するユーザ処理OSであり、前記第2のOSは前記ネットワーク部を介して前記ハードデ

ィスク装置と前記暗号化された前記データの通信を実施する通信処理OSであることを特徴とする、上記(1)に記載の計算機。

【0031】図3は本発明の実施の形態におけるハードディスク装置100で動作するソフトウェアの構成を示したものである。ハードディスク装置100では、ストレージOS300が動作する。ストレージOS300上で、各計算機からのプリブート/リモートブート要求を処理するリモートブート処理301、各計算機を使用する使用者の認証を行う認証プログラム302、及び、各計算機との通信処理を行う通信処理303が動作する。また、ストレージOS300は、各計算機の実行に必要なプログラムとデータを格納するストレージデバイスを制御するためのディスク管理処理305と、LAN-A140を経由して各計算機と通信を行うためのネットワーク処理306を備える。ハードディスクデバイス104は、いくつかの領域に分かれている。当該領域において、各計算機をネットワークブートするための、ブートローダプログラム307と、使用者毎のOS、アプリケーションプログラムとユーザデータを格納するための領域を有する。使用者A用領域308、使用者B用領域309、使用者C用領域310は当該領域に含まれる。

【0032】また、各ソフトウェア処理は、処理に必要なデータもハードディスクデバイス104に格納している。さらに、ハードディスク装置100内には使用者情報311、計算機情報312、鍵データ313、及びマップ情報314が備えられている。使用者情報311はハードディスク装置100に格納されたプログラム/データへのアクセスを認められた使用者を管理する情報である。同様に計算機情報312はアクセスを認められた計算機を管理する情報である。鍵データ313は各計算機とハードディスク装置100の間の通信データを暗号処理304で暗号化する場合に必要な鍵データを格納する。又、マップ情報314はアクセスが認められた使用者/計算機とハードディスクデバイス104の領域の対応関係を格納する。

【0033】本発明の図3に示すソフトウェアの構成に基づき、動作する図1のハードディスク装置100は、以下の項目(i)から(vii)の特徴を備えるハードディスク装置として提供しうる。

【0034】(i) CPU、メモリ、ハードディスクユニット及びネットワーク部を備えるハードディスク装置から構成され、前記CPUはブート処理部、認証プログラムユニット、通信処理部及び前記ハードディスクユニットを制御するディスク管理部を含み、前記通信処理部は、暗号処理ユニット及び鍵生成データを備え、前記認証プログラムユニットは前記ネットワーク部を介して接続されている複数の計算機の各々が有するハードウェア情報及び前記計算機を管理する使用者情報を保持し、前記ハードディスクユニットは複数の領域を備え、該複数の

領域には前記複数の計算機毎の前記ハードウェア情報が格納され、前記暗号処理ユニットは、前記計算機から送信されるブート要求を前記ブート処理部にて処理した後、前記鍵生成データに基づき鍵データを作成し、前記ハードウェア情報に前記鍵生成データ或いは鍵データを付加して前記ブート要求を発信した前記計算機に対し配信することを特徴とするハードディスク装置。

【0035】(ii) 前記ハードウェア情報は前記計算機毎に格納されているユーザ処理OS、通信処理OS、及びユーザにより利用されるアプリケーションプログラムを含み、前記使用者情報はユーザを識別する為の認証情報であることを特徴とする、上記(i)に記載のハードディスク装置。

【0036】(iii) 前記認証情報は、前記計算機を使用するユーザ名、該ユーザのパスワード、及び該ユーザが利用しているデータ格納用ディスクの情報であることを特徴とする、上記(ii)に記載のハードディスク装置。

【0037】(iv) 前記鍵データは前記暗号処理ユニットが備える鍵データ部において作成され、前記鍵データ部は計算機を識別する為の固有データ及び暗号化情報を保持することを特徴とする、上記(i)に記載のハードディスク装置。

【0038】(v) 前記固有データ及び暗号化情報は前記計算機のネットワークアドレス、前記鍵生成データ、前記鍵データ、及び前記鍵データの生成時間を含む情報であることを特徴とする、上記(iv)に記載のハードディスク装置。

【0039】(vi) 前記ディスク管理部の制御に従い、前記計算機から前記送信される暗号化された通信データを前記通信処理部が処理し、前記ハードディスクユニットが有する前記複数の領域の内、何れかの領域に前記暗号化された通信データを格納することを特徴とする、上記(i)に記載のハードディスク装置。

【0040】(vii) さらに、前記ディスク管理部の制御に従い、前記計算機から送信される前記暗号化された通信データを前記暗号処理ユニットが有する前記鍵データを使用し、暗号化されていない元データに戻し、前記複数の領域の内、何れかの領域に該元データを格納することを特徴とする、上記(vi)に記載のハードディスク装置。

【0041】図4から図7は、データの構造を示したテーブルである。当該テーブルは、前記ハードディスクデバイス104に格納されたハードディスク100で動作するソフトウェア300、301、302、303が使用する。ここでソフトウェア300、301、302、303は各々ストレージOS300、リモートブート処理301、認証プログラム302、通信処理303に該当する。

【0042】図4は、使用者情報311の詳細を示した

テーブル構造である。使用者情報311は、使用者の名前を格納する使用者名400、使用者を認証するためのパスワード401、及び、使用者が割り当てられたハードディスクデバイス104の領域を示すデータディスク情報402で構成される。

【0043】図5は、計算機情報312の詳細を示したテーブル構造である。計算機情報312は、計算機を識別するための名称を格納した計算機名500、各計算機のネットワークデバイスA114毎の固有のハードウェア情報であるMACアドレス501、及び、各計算機の構成情報から求めたハードウェア情報502で構成される。ハードウェア情報502は、各計算機のCPU111のクロック性能とメモリA112とメモリB113の搭載メモリサイズの合計値から計算で求めた値を使用するものとする。ここで、MACはMedia Access Controlに該当する。

【0044】図6は、マップ情報314の詳細を示したテーブル構造である。マップ情報314は、使用者が使用する計算機と計算機が必要とするハードディスク領域の対応を格納するテーブルである。当該マップ情報314は、使用者情報311から得られたディスク情報402と、計算機情報312から得られたMACアドレス501を格納している。

【0045】図7は鍵データ313の詳細を示したテーブル構造である。鍵データ313は、各計算機を識別するために、計算機情報312から得られるMACアドレス501を格納し、MACアドレス501毎に鍵データを管理する。鍵データ313のテーブルは、暗号化するための鍵データを生成するための鍵生成データ700を格納する。さらに、鍵生成データ700から生成し、通信データの暗号化に用いる鍵データ701を格納している。そして、鍵データ701を生成した生成時間702を格納する。鍵生成データ700は計算機毎に異なる値が設定される。さらに生成した鍵データは生成時間を管理する。又、一定時間ごとに鍵生成データ700から鍵データ701を生成し、暗号化に用いる鍵データを変更することによって、通信データの安全性を高める。

【0046】図8(a)、(b)は、図1に示す各計算機110、120、130とハードディスク装置100のプログラム起動手順を示すフローチャートである。

【0047】プログラム起動手順では、まず、計算機110、120、130の電源がオンになると(ステップ800)、ブート制御回路117が起動し、ネットワークデバイスA114を使用して、LAN-A140のネットワークに対して、プリブート/リモートブートを要求する(ステップ801)。

【0048】LAN-A140上のプリブート/リモートブートの要求は、ハードディスク装置100内のリモートブート処理301(図3)が受け付ける。リモートブート処理301は、計算機情報312を参照し、プリ

ブート/リモートブートを要求している計算機の計算機名500(図5)とMACアドレス501を比較する(ステップ802)。テーブルに格納されている計算機の場合は、ブートローダプログラム307を要求元の計算機に送信する(ステップ803)。

【0049】次に、要求元の計算機は、ハードディスク装置100から送信されたブートローダプログラム307を実行し、入出力デバイス116により、使用者の使用者名とパスワードを確認する(ステップ804)。また、当該計算機は使用者が使用している計算機のCPU111のクロック性能とメモリA112とメモリB113の搭載メモリサイズの合計値を組み合わせた値(ハードウェア情報502)を計算する(ステップ805)。その後、計算機は認証データとして、使用者名、パスワード、ハードウェア情報の3つを、ハードディスク装置100に送信する(ステップ806)。

【0050】次に、ハードディスク装置100内の認証プログラム302は、送信された認証データと使用者情報311(図4)の使用者400、パスワード401、及び計算機情報312(図5)の計算機名500、MACアドレス501、ハードウェア情報502を比較する。使用が認められている使用者/計算機の場合は、MACアドレス501とディスク情報402をマップ情報314(図6)に格納する(ステップ807)。また、要求元の計算機との通信データを暗号化するための鍵生成データ700を作成し、対応するMACアドレスと作成した鍵生成データ700を鍵データ313のテーブル(図7)に格納する(ステップ808)。また、生成した鍵生成データ700は、使用者のハードディスク領域における鍵生成用データ210(図2)の格納エリアにも書き込みを行う(ステップ809)。鍵生成用データ210が書き込まれたハードディスク領域104にあるユーザ処理OS200、通信処理OS201、複数OS処理202が、要求元の計算機に送信される(ステップ810)。

【0051】次に、要求元の計算機は、送信された上記OS200、201、202を起動し(ステップ811)、引き続き、通信処理OS201上で動作する通信処理、ユーザ処理OS200上で動作するアプリケーションプログラムの順で起動処理を行う(ステップ812)。

【0052】以上により、計算機上のプログラムの起動は完了する。先に述べたように、アプリケーションプログラムによるディスクに対するアクセス要求は、実施される。当該アクセス要求は図2に示す仮想ディスク処理207、通信処理205により、ハードディスク装置100に送られ、各計算機からのハードディスクへのアクセスが実現できる。

【0053】さらに、各計算機110、120、130とハードディスク装置100間の通信データを暗号化す

る場合は、通信データの暗号化に必要な鍵生成データ 210、700は、上記ステップ808において、ハードディスク装置内にて各計算機毎に作成される。さらに、鍵生成データから鍵データが生成される。上記ステップ810において、図8(b)のフローチャートに示すようにステップ810-1及び810-2にて、各計算機にもネットワークブート時に鍵生成データ、或いは鍵データが送信されている。そのため、図8(a)に示したステップ812の手順以降のアプリケーションプログラムによるディスクに対するアクセスに用いられる通信データを暗号化できる。

【0054】上述した本発明の図8に示すプログラム起動手順を示すフローチャートに従い、プログラムが起動される図1のディスク装置共有システムにおいて、各計算機110、120、130がハードディスク装置100を共有する方法は、以下の項目(1)から(4)の特徴を有するディスク装置の共有方法として提供可能である。

【0055】(1)複数の計算機と、該複数の計算機により共用されるハードディスク装置と、該複数の計算機と前記ハードディスク装置がネットワークにより相互接続される計算機システムにおいて、前記計算機システムがブート処理するステップと、前記ブート処理の後、前記計算機はユーザによる認証IDの入力後、認証データを作成し前記ハードディスク装置に対し、送信するステップと、前記ハードディスク装置にて前記認証データの認証処理を実施し、前記複数の計算機に対し、前記ハードディスク装置が備える暗号処理部が鍵データを作成するステップと、前記計算機の実行に必要と成るオペレーティングシステム、前記ユーザにより利用されるアプリケーションソフトと共に前記鍵データを前記計算機に対し配信するステップとを含むことを特徴とするディスク装置の共有方法。

【0056】(2)前記ハードディスク装置は、鍵生成データ及び鍵データ部を備え、前記作成するステップにおいて、前記鍵生成データに基づいて前記鍵データが作成され、前記鍵データ部は前記複数の計算機と前記ハードディスク装置間の通信データを前記暗号処理部にて暗号化する際に必要な前記鍵データを格納することを特徴とする、上記(1)に記載のディスク装置の共有方法。

【0057】(3)前記オペレーティングシステムは、ユーザ処理OS及び通信処理OSを含み、前記配信するステップにおいて、前記計算機に対し、前記鍵生成データ或いは鍵データが前記オペレーティングシステム及びアプリケーションソフトと共に送信されることを特徴とする、上記(2)に記載のディスク装置の共有方法。

【0058】(4)さらに前記鍵データを用いて、前記計算機は前記ユーザにより利用されるアプリケーションソフトを実行した結果、得られるデータを暗号化し前記ハードディスク装置に対し前記ネットワークを介して転

送するステップを含むことを特徴とする、上記(1)に記載のディスク装置の共有方法。

【0059】以上説明した実施形態によれば、計算機にはプログラムやデータを保存するためのハードディスクデバイスを備えることなく、ネットワーク上のハードディスク装置にプログラムやデータを保存できる。アプリケーションプログラムやOSなどのインストールやバージョンアップ、並びにデータのバックアップを一元管理することができる。従って運用管理コストを低減しTCOの低い計算機システムを実現できるという効果がある。

【0060】また、本実施形態によれば、一台の計算機上にOSを2つ搭載することによって、アプリケーションプログラムを実行するOSと、共有するハードディスク装置との通信処理を実行するOSとの機能分担を実現できる。これにより、インターネット等の外部ネットワークとハードディスク装置に対するアクセスを実現するための内部ネットワークを分離することができる。それ故、外部ネットワークから不正なプログラムにより、アプリケーションプログラムを実行するOSの管理者権限が奪われても、独立した通信処理を実行するOSが設けられる為、不正なプログラムは内部ネットワークに侵入できない。従って、共有するハードディスク装置の安全性を高めることができる。

【0061】また、本実施形態によれば、計算機とハードディスク装置間の通信データを暗号化する場合、暗号化に必要な鍵データを生成する為のデータが、計算機をネットワークブートする段階で配布される。従って、事前に計算機に保存する必要がなく、計算機のハードウェアの解析によって、暗号化のためのデータを盗まれないという効果がある。ネットワークブートする段階で配布する鍵生成データは、アプリケーションプログラムを実行するOSから独立したもうひとつのOSである通信処理を実行するOS側に保存することによって、外部ネットワークから不正なプログラムにより、アプリケーションプログラムを実行するOSの管理者権限が奪われても、鍵生成データを守ることができる。

【0062】

【発明の効果】以上に示すように本発明に依れば、複数の計算機と共用ハードディスク装置がネットワークを介して相互接続される環境において、安全なデータ通信を実現し、計算機のメンテナンスに要する運用コストの低減を実現するディスク装置共有システムを提供する事が出来る。

【図面の簡単な説明】

【図1】本発明の一実施例におけるディスク装置共有システムを使用した計算機環境の構成を示すシステム構成図である。

【図2】図1に示す計算機上で動作するソフトウェアの構成図である。

【図3】図1に示すハードディスク装置上で動作するソフトウェアの構成図である。

【図4】使用者情報テーブルのデータ構造を示す図である。

【図5】計算機情報テーブルのデータ構造を示す図である。

【図6】マップ情報テーブルのデータ構造を示す図である。

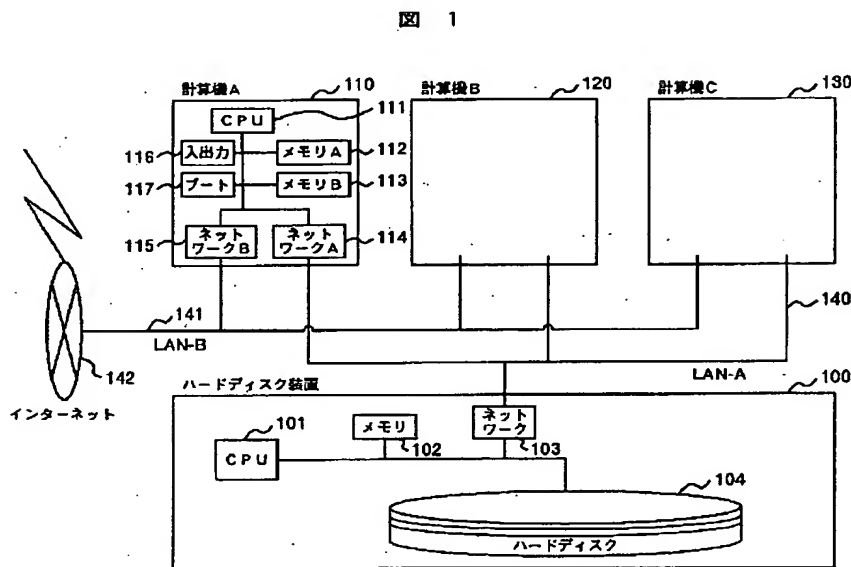
【図7】鍵データテーブルのデータ構造を示す図である。

【図8】図8(a)は、本発明の図1に示すシステム構成において計算機のブート処理手順を示すフローチャートであり、図8(b)は、図8(a)が示すフローチャートにおけるプログラムの転送処理の詳細フローを示す図である。

【符号の説明】
100…ハードディスク装置、101…CPU、102…メモリ、103…ネットワークデバイス、104…ハードディスクデバイス、110…計算機、111…CPU、112…メモリ、113…メモリ、114…ネットワークデバイス、115…ネットワークデバイス、116…入出力、117…ブート、118…ネットワークデバイス、119…ネットワークデバイス、120…計算機、130…計算機、140…ネットワーク、141…ネットワーク、142…インターネット。

【図1】

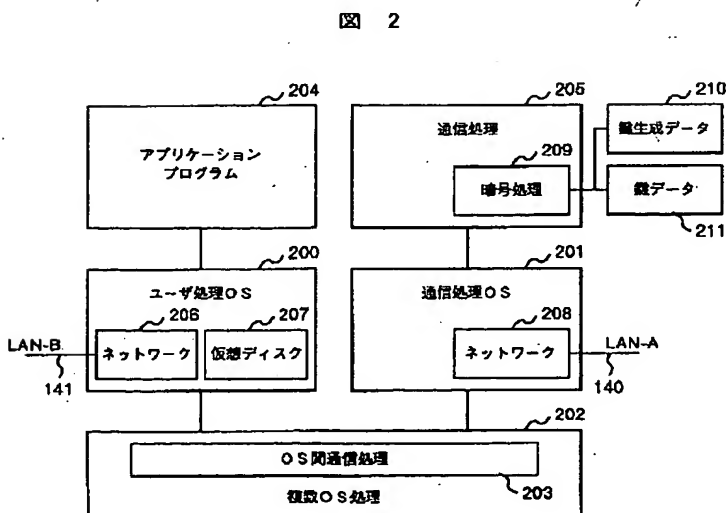
【図6】



314	501	402
MAC アドレス	ディスク情報	
MAC-A	DISK-A	
MAC-B	DISK-B	
MAC-C	DISK-C	

【図2】

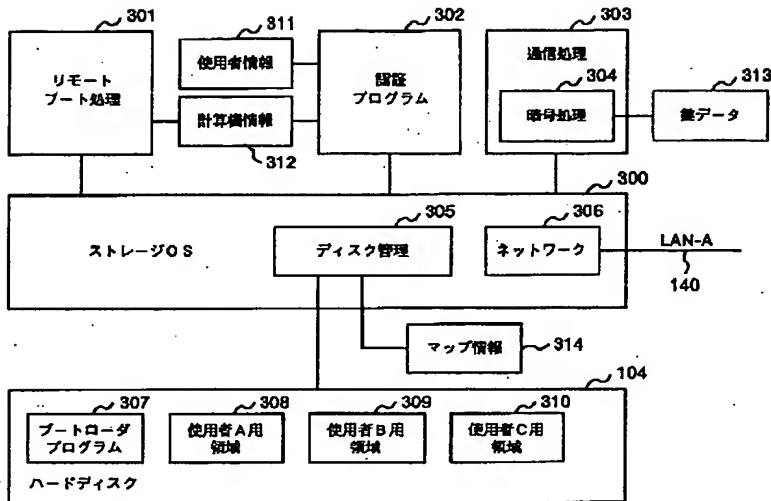
【図4】



311	400	401	402
使用者名	パスワード	ディスク情報	
使用者A	*****	DISK-A	
使用者B	*****	DISK-B	
使用者C	*****	DISK-C	

【図3】

図 3



【図5】

図 5

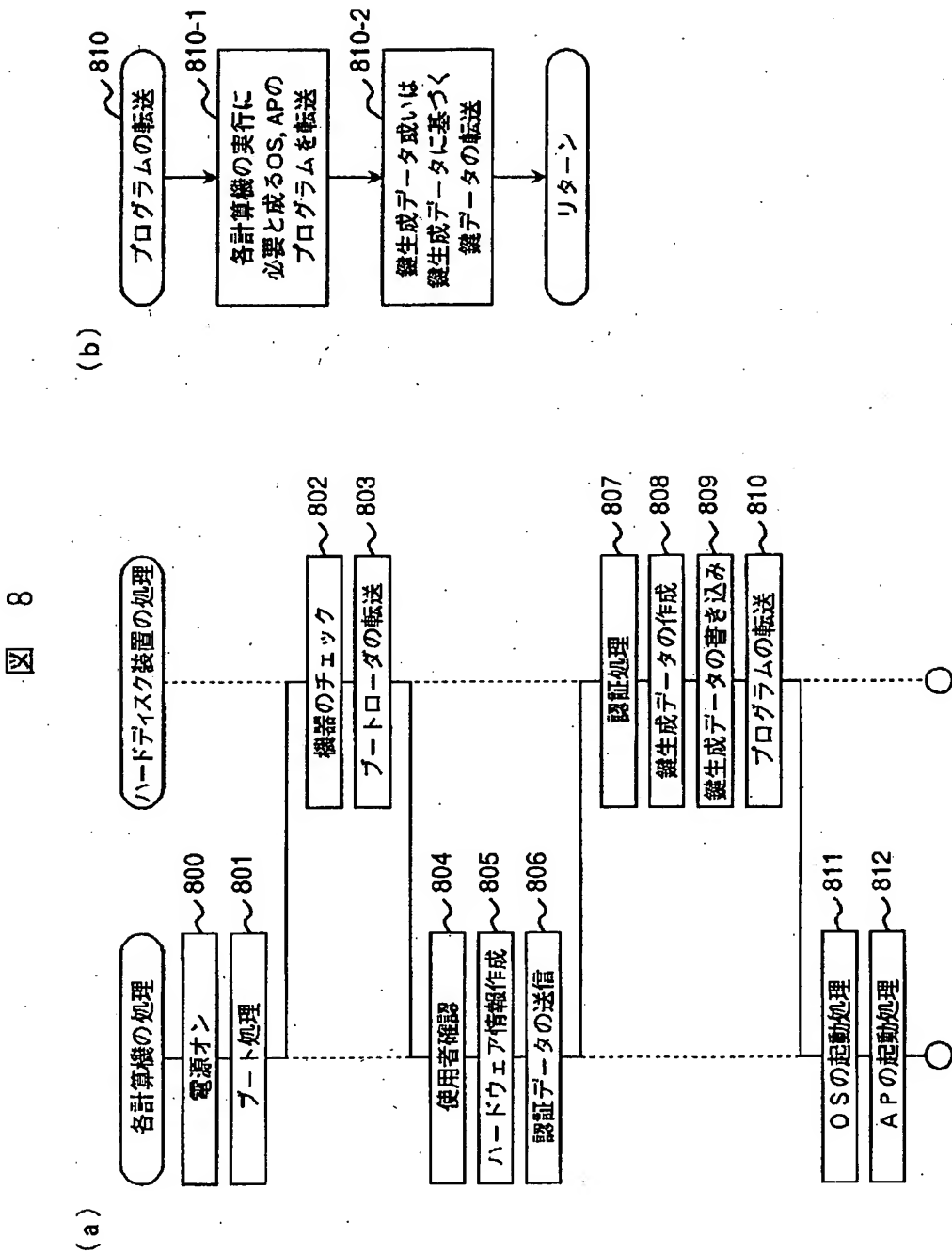
312 計算機名	500 MAC アドレス	501 ディスク情報
計算機 A	MAC-A	933MH512MB
計算機 B	MAC-B	733MH256MB
計算機 C	MAC-C	933MH512MB

【図7】

図 7

313 MAC アドレス	501 鍵生成データ	700 鍵データ	701 生成時間
MAC-A	1HjzoL	*****	12:23:59
MAC-B	kOf4x	*****	10:41:12
MAC-C	uT5bq	*****	21:35:42

【図8】



フロントページの続き

(72)発明者 佐藤 雅英
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 大島 訓
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

Fターム(参考) 5B017 AA03 BA07 CA07
5B065 BA01 CA02 CC08 PA16
5B082 FA16 GA11
5J104 EA15 NA30 PA14